書名：密碼學(九章出版社出版)

作者：霍安琪

內容簡介：

根據歷史學家的研究，密碼學的起源可以追溯至約四千多年前尼羅河岸一帶；自此之後，更加複雜的加密法慢慢演變出來，作為政治及軍事用途。電腦在二十世紀改變了人類的生活模式，密碼學最常見的應用便是在互聯網上保障資料的安全傳送，例如電子商貿及電郵通訊等。在林林總總曾經被廣泛使用的密碼系統背後，往往離不開數學原理，而一些現正在互聯網上使用的系統，更應用了數百年前甚至二千多年前早已被証明的數學定理。

密碼學的發展十分令人著迷，密碼設計者和密碼分析員之間的智力競賽極為緊張刺激；數學理論和現代密碼學配合得天衣無縫，深深吸引著人們動手研究的興趣。本書深入淺出地介紹各種較為知名的系統，以及一些有關的知識；從單表代替密碼、多表代替密碼、編碼系統、數據加密標準(DES)、交換密鑰協議以及 RSA 等。作者以書中精彩有趣的內容，帶領讀者進入奧妙的密碼世界。

心得：

生活在二十一世紀的今天，電腦明顯地成為我們生活中的一部分，為了保障資料在網路上傳送的隱密性，就必須使用密碼；密碼

不僅有助於避免有人非法獲得與他毫無關係的數據，而且可使每位公民能與他人交換秘密訊息；一些人認為這是公民的正當權利，菲力浦・齊默爾曼，PGP 密碼程式的發明者，就是其中之一。但是商人們能借用密碼交流訊息，這能將商業機密保密，但卻不會危害國家的公益；另一方面，犯罪組織以及與國家敵對的組織也能使用密碼，因此黑手黨就能從哥倫比亞出發借用網路安排下一批貨的運輸路線，而右派或左派恐怖份子則能從網路上獲悉下一次聚眾鬧事的時間和地點，這就對國家造成了不小的打擊。有些國家的政府考慮限制民間使用他們也無法破解的密碼系統，究竟這樣做是否合宜，只能留待歷史去解答。

另一方面，雖然密碼保障我們通訊上的隱私，相對的，我們卻可以由此得知人性的黑暗：總是有人不斷的想探知別人的隱私，甚至於拿來討論；由於密碼的使用，造成了人與人之間更多的猜忌；人們的道德層次真的如此低落嗎？人類已如此墮落嗎？古時候曾經有過路不拾遺、夜不閉戶的紀錄，現今要做到這樣只有兩種方法：1.提昇道德層次 2.重法，但兩種方法似乎都離現實太遠……。人需要彼此猜忌、彼此懷疑嗎？道家所謂：「智慧出，有大偽。」歷史似乎證實了這句話；由密碼學發展而看見的人性黑暗面，值得我們深思！

研究：

一.質數產生法：

一般而言，有兩種方法可以產生大的質數，一為機率式質數測試法，另一為確定式質數測試法。

1.Miller-Rabin 機率式質數測試法：

令輸入 n 為正奇數，且 $n = 2^s + 1$，其中 $s \geq 1$，且 t 為奇數。

(1)任選一正整數 a 並測試 a 是否滿足

(Ⅰ) $a^t \neq 1 \pmod{n}$；

(Ⅱ) $a^{2jt} \neq -1 \pmod{n}$　　$0 \leq j \leq s-1$

若 a 滿足條件(Ⅰ)(Ⅱ)，則 n 必為合成數(根據費馬定理)；

否則，稱 n 通過一次測試，即 n 可能為質數。

(2)重複步驟 1，任意選擇不同的 a 共 k 次，以進行測試。

2.確定式質數測試法

(1)此為 Lucas 在 1876 年所提的方法：

若 n 滿足 $b^{n-1} = 1 \pmod{n}$且 $b^{(n-1)/pi} \neq 1 \pmod{n}$；

其中 b 為任意正整數，p_i 為每一$(n-1)$之質因數，

即 $p_i \mid (n-1)$，則 n 必為質數。

(2)此為 Demytko 在 1988 年所提的方法：

$p_{i+1} = h_i p_i + 1$ 若滿足下列條件，則 p_{i+1} 必定為質數：

(Ⅰ)p_i為一奇質數；

(Ⅱ)$h_i < 4(p_i + 1)$，且h_i為偶數；

(Ⅲ)$2^{hipi} = 1 \pmod{p_{i+1}}$；

(Ⅳ)$2^{hi} \neq 1 \pmod{p_{i+1}}$。

二.歐拉定理(Euler´s Theorem)：

當 a,n 為正整數，$(a,n) = 1$，則 $a^{\varphi(n)} = 1 \pmod{n}$

$\varphi(n)$代表比 n 小且同時與 n 互質的正整數數目。

考慮 mod n 的一個縮系

$$b_1, b_2, b_3, \cdots, b_{\varphi(n)} \qquad (Ⅰ)$$

用 a 去乘它們得

$$ab_1, ab_2, ab_3, \cdots, ab_{\varphi(n)} \qquad (Ⅱ)$$

因為(Ⅰ)(Ⅱ)皆是 mod n 的縮系

故 $ab_1ab_2ab_3\cdots ab_{\varphi(n)} \equiv b_1b_2b_3\cdots b_{\varphi(n)} \pmod{n}$

約去 $b_1b_2b_3\cdots b_{\varphi(n)}$得

$$a^{\varphi(n)} = 1 \pmod{n}$$

三.密鑰中心衍生 RSA 密鑰的過程：

(Ⅰ)選擇 2 個很大且並不相等的隨機質數 p 和 q，

每一個約為 200 位的十進數。

(Ⅱ)計算 $n = pq$ 和 $\varphi(n) = (p-1)(q-1)$

(n 一般為強質數，即存在兩質數 p 和 q，使得 p|(n－1),

q|(n + 1)；存在四質數 r, s, t, u 使得 r|(p + 1), s|(p－1),

t|(q + 1), u|(q－1))

(Ⅲ)選擇一個很大的隨機數 d，(d, φ(n)) = 1

(Ⅳ)計算 1 < e < φ(n)使得 ed $\equiv$ 1 (mod φ(n))。

(Ⅴ)公佈<n,e>作為公開鑰，分發 d 作為私有鑰，

銷毀 p 和 q 的值，不予紀錄。

四.(1)若能分解因數 n，即能破解 RSA 系統

證明(Ⅰ)：若能分解因數 n，即可知

n = pq 及 φ(n) = (p－1)(q－1)

則可得出唯一的 d´，使得 ed´ $\equiv$ 1 (mod n)且 1 < d´ < φ(n)

利用 Euler´s Theorem 我們可證明

若 C $\equiv$ W^e (mod n)則 $W \equiv C^{d'}$ (mod n)，

其中 ed´ $\equiv$ 1 (mod φ(n))。

∵ ed´ $\equiv$ 1 (mod φ(n))

ð φ(n)|(ed´- 1)

ð ed´- 1 = kφ(n)對於某正整數 k。

情況一：p 和 q 都不整除 W，即(W,n) = 1

由 Euler´s Theorem 得出 $W^{\varphi(n)} \equiv 1$ (mod n)

ð $W^{ed'-1} \equiv W^{k\varphi(n)} \equiv 1^k \equiv 1 \pmod{n}$

ð $W^{ed'} = W^{ed'-1}W \equiv 1 \cdot W \equiv W \pmod{n}$

ð $C^{d'} \equiv W \pmod{n}$。

情況二：p 可整除 W 但 q 不可，即(W,q) = 1

由費馬小定理得出 $W^{q-1} \equiv 1 \pmod{q}$

ð $W^{\varphi(n)} \equiv W^{(p-1)(q-1)} \equiv 1^{p-1} \equiv 1 \pmod{q}$

ð $W^{ed'-1} \equiv W^{\varphi(n)} \equiv 1^k \equiv \pmod{q}$

ð $W^{ed'} = W^{ed'-1}W \equiv 1 \cdot W \equiv W \pmod{q}$

ð $C^{d'} \equiv W \pmod{q}$

ð $C^{d'}$ - W 可被 q 整除。

另一方面由於 p 整除 W

ð $W \equiv 0 \pmod{p}$

ð $W^{ed'} \equiv 0 \pmod{p}$

ð $W^{ed'} \equiv W \pmod{p}$

ð $C^{d'} \equiv W \pmod{p}$

ð $C^{d'}$ - W 可被 p 整除。

所以 $C^{d'}$ - W 同時可被 p 和 q 整除，亦即可被 n = pq 整除。

$\therefore C^{d'} \equiv W \pmod{n}$。

情況三：p 和 q 同時可整除 W。

在情況二中可見當 p 整除 W 時，$C^{d'} - W$ 亦可被 p 整除，

同樣地，由於 q 整除 W，所以 $C^{d'} - W$ 亦可被 q 整除，

因此 $C^{d'} - W$ 可被 $n = pq$ 整除。

$\therefore C^{d'} \equiv W \pmod{n}$。

更一般的，我們說：$d = d' + t\varphi(n)$　　(t 為整數)

證明(Ⅱ)：由於 d 是 RSA 系統的私有解密鑰,故 $ed \equiv 1 \pmod{\varphi(n)}$

由證明(Ⅰ)可知：d′亦可作為 RSA 系統的解密鑰，

又$\because ed \equiv 1 \pmod{\varphi(n)}$,

$\therefore ed - 1 = s\varphi(n)$　　(s 為整數)

令 $s = k + et$，得 $ed' - 1 = k\varphi(n)$

ð $ed' - 1 + et\varphi(n) = k\varphi(n) + et\varphi(n)$

ð $ed' + et\varphi(n) - 1 = (k + et)\varphi(n) = s\varphi(n)$

ð $e(d' + t\varphi(n)) - 1 = s\varphi(n)$

ð $ed - 1 = s\varphi(n)$

ð 故 $d = d' + t\varphi(n)$

故若能分解因數 n，即能得到與密鑰同效的數字 d′，也就破解了 RSA 系統。

(2)若能破解 RSA 系統，即能分解因數 n (？)

A：相信，但尚未有證明。

因為若能破解 RSA 系統，即可知 $ed' - 1 \equiv 0 \pmod{\varphi(n)}$

$\eth$ $ed' - 1 = k\varphi(n)$　　(k 為任意正整數)

再分解因數 $k\varphi(n)$，刪去非 4 之倍數的因數

(∵ p,q 為奇數 ∴ $2|(p-1)$, $2|(q-1)$

$\eth$ $4|(p-1)(q-1)=\varphi(n)$)

如能分解因數 $\varphi(n)$ 並求出 $(p-1)$ 及 $(q-1)$，則可分解因數 n，

不過由於 RSA 系統使用強質數，故由 $\varphi(n)$ 求 p 及 q 亦非常困難，

故目前相信若能破解 RSA 系統，則能分解因數 n，但至今未有人給出證明。

參考書目：

1.密碼學　霍安琪著　九章出版社

2.近代密碼學及其應用　賴溪松、韓亮、張真誠著　旗標出版社

3.趣味數論　單墫著　九章出版社

13028 陳雲昶